(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 519 581 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
30.03.2005 Bulletin 2005/13

(51) Int Cl.[7]: **H04N 7/167**, H04L 29/06

(21) Application number: **04255786.8**

(22) Date of filing: **22.09.2004**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL HR LT LV MK

(30) Priority: **26.09.2003 US 506193 P**
21.01.2004 US 762680

(71) Applicant: **Genesis Microchip, Inc.**
Alviso, CA 95002 (US)

(72) Inventor: **Kobayashi, Osamu**
Los Altos CA 94024 (US)

(74) Representative: **Alton, Andrew**
Urquhart-Dykes & Lord LLP
Tower North Central
Merrion Way
Leeds LS2 8PA (GB)

(54) Packet based high definition high-bandwidth digital content protection

(57) A packet based high bandwidth copy protection method is described that includes the following operations. Forming a number of data packets at a source device, encrypting selected ones of the data packets based upon a set of encryption values, transmitting the encrypted data packets from the source device to a sink device coupled thereto, decrypting the encrypted data packets based in part upon the encryption values, and accessing the decrypted data packets by the sink device.

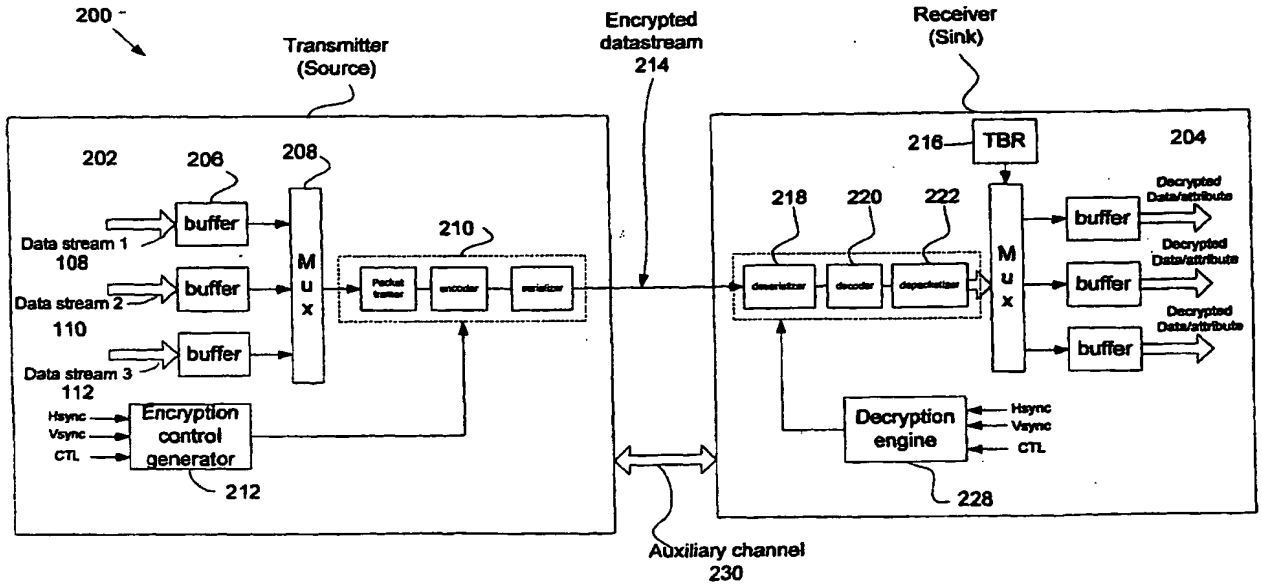

Fig. 2

EP 1 519 581 A1

Description

[0001] The invention relates to display devices. More specifically, the invention describes a method and apparatus capable of providing a robust encryption of a audio/video data in a packet based transmission environment.

[0002] Protection of proprietary digital content has become an important consideration and more particularly, in high definition (HD), high-bandwidth applications. Especially important for HD, high-bandwidth applications, content protection provides assurances that owners of digitized content are protected from unauthorized use and copying of their proprietary content. A popular high-bandwidth digital-content protection scheme developed by Intel Corporation of Santa Clara CA commonly referred to as HDCP has been widely implemented. As currently configured, this particular HDCP protocol is specifically designed for use in Digital Visual Interface (DVI) and High-Definition Multimedia Interface (HDMI) based environments.

[0003] In general, HDCP encrypts the transmission of digital content between the video source, or transmitter -- such as a PC, DVD player or set-top box -- and the digital display, or receiver – such as a monitor, television or projector. In this way, HDCP is designed to prevent copying or recording of digital content thereby protecting the integrity of content as it is being transmitted. For example, as required by the described HDCP protocol, during an authentication phase, the receiver will only be provided with content once it demonstrates knowledge of the authentication keys which the transceiver verifies through computation of a secret value. Furthermore, to prevent eavesdropping and stealing of the data, the transmitter and receiver will generate a shared secret value that is consistently checked throughout the transmission. Once authentication is established, the transmitter encrypts the data and sends it to the receiver for decryption.

[0004] The current implementation of the DVI standard requires the use of a set of defined characters based upon a 10 bit transmission protocol. For example, as currently configured, only 460 characters (out of a possible 1024 available) are used by the receiver for data while 4 characters are used as explicit control signals such as hsync and vsync. In this arrangement, any time the receiver receives and recognizes one of the predefined characters representing data, then the received implicitly defines a data enable signal (DE) as being active thereby indicating that the received data is true data. However, whenever one of the 4 control characters is received by the receiver, then an implicit assumption is made that data enable (DE) is inactive.

[0005] HDCP protocol uses the status of DE, H_{sync}, V_{sync} and another control signal, called CNTL3, to advance its state machine. The DE, H_{sync}, and V_{sync} signals are timing signals associated with raster video transmitted in a "streaming" manner. In a streaming transfer, the pixel data is transferred at pixel rate and the ratio of blanking period to data period is preserved. In case of a packet transfer, these timing signals may not be present. Only the pixel data may be transferred in the packet stream, while timing information is communicated in a different way. Therefore, what is required is a way to support high-definition copy protection that is compatible with existing high definition copy protection protocols such as HDCP over a link, or a transmission medium, that operates in a packet transfer mode.

[0006] What is provided, therefore, is a packet-based digital transmission medium and protocol that supports high definition copy protection that is backwards compatible with existing high definition copy protection protocols such as HDCP.

[0007] In one embodiment of the invention, a packet based high bandwidth copy protection method is described that includes the following operations. Forming a number of data packets at a source device, encrypting the data packets based upon a set of encryption values, transmitting the encrypted data packets from the source device to a sink device coupled thereto, decrypting the encrypted data packets based in part upon the encryption values, and accessing the decrypted data packets by the sink device.

[0008] In another embodiment, a system for providing packet based high bandwidth copy protection to a data stream is disclosed that includes a source unit arranged to provide a number of data packets, a sink unit coupled to the source unit arranged to receive the data packets from the source unit, an encryption unit coupled to the source unit arranged to encrypt the data packets sent from the source unit to the sink unit, a decryption unit coupled to the sink unit arranged to decrypt the encrypted data packets and an encryption/decryption values generator arranged to provide a set of encryption/decryption values used to encrypt and decrypt the appropriate data packets.

[0009] In yet another embodiment, computer program product for providing a packet based high bandwidth copy protection is disclosed that includes computer code for forming a number of data packets at a source device, computer code for encrypting the data packets based upon a set of encryption values, computer code for transmitting the encrypted data packets from the source device to a sink device coupled thereto, computer code for decrypting the encrypted data packets based in part upon the encryption values, computer code for accessing the decrypted data packets by the sink device, and computer readable medium for storing the computer code.

[0010] An embodiment of the invention will now be described in detail, by way of example only, and with reference to the accompanying drawings, in which:

Fig. 1 shows a generalized representation of a cross platform packet based digital video display interface suitable for use with any embodiment of the

invention;

Fig. 2 shows an encryption system for encrypting audio/video content suitable for use with the system described with respect to Fig. 1;

Fig. 3 shows a representative encrypted data stream in accordance with an embodiment of the invention; and

Fig. 4 illustrates a system employed to implement the invention.

[0011] Reference will now be made in detail to a particular embodiment of the invention an example of which is illustrated in the accompanying drawings. While the invention will be described in conjunction with the particular embodiment, it will be understood that it is not intended to limit the invention to the described embodiment. To the contrary, it is intended to cover alternatives, modifications, and equivalents as may be included within the spirit and scope of the invention as defined by the appended claims.

[0012] As currently implemented, HDCP establishes a secure channel in order to verify that the display device is licensed to receive protected content and once established, encrypts the data at the host side and decrypts at the display device in order to prevent 'eavesdropping' of the protected content. In addition, in order to identify unauthorized or comprised devices, HDCP relies upon authentication and key exchange, content encryption, and device renewability.

[0013] More specifically, HDCP protects copyrighted digital entertainment content in a Digital Video Interface (DVI) environment by encrypting its transmission between the video source and the digital display (receiver). The video source might be a PC, set-top boxes, DVD players and the like), and the digital display might be an liquid crystal display (LCD), television, plasma panel, or projector in which all authorized devices are given a set of unique secret device keys. During an authentication process, the receiver must demonstrate its knowledge of a number of secret device keys before the protected content is sent. After the receiver acknowledges the keys, both devices (the sender and receiver) generate a shared secret value that is designed to prevent eavesdroppers from stealing the content. After authentication, the content is encrypted and sent to the receiver that in turn decrypts it.

[0014] Authentication is a cryptographic process for verifying that the display device is authorized (or licensed) to receive protected content. Both the authorized host and the display device have knowledge of a set of secret keys that consist of an array of forty 56-bit secret device keys and a corresponding 40-bit binary Key Selection Vector (KSV). The host initiates authentication by sending an initiation message containing its Key Selection Vector, AKSV, and a 64-bit value An. The display device responds by sending a response message containing its Key Selection Vector, BKSV. The host confirms that the received KSV has not been revoked. At this point, the two devices can calculate a shared value, which, if both devices have a valid set of keys, will be equal. This shared value will be used in the encryption and decryption of the protected content since authentication has now been established.

[0015] Re-authentication continues at a rate of approximately once every two seconds to confirm the continued security of the link. If, at any time, equality of the shared value is lost, for example by disconnecting the display device and/or connecting an illegal recording device, the host will consider the DVI link to be unauthenticated, and end the transmission of protected content.

[0016] Content is encrypted at the source device to prevent usable, unauthorized copies of the transmitted content from being made. Encryption is the application of an algorithm, called a cipher, that transforms the content. To recover the content, the display device decrypts the content by knowledge of the correct decryption key. The HDCP cipher is a hybrid block/stream cipher. The block cipher operates during the authentication protocol. For content encryption and decryption, HDCP uses a stream cipher where encryption is accomplished by combining a data stream, generated by the HDCP cipher, with the transmitted content, through a bitwise exclusive-OR operation. In this way the content is protected pixel-by-pixel. Encrypted content viewed on a display device without decryption is seen as random noise, with no discernable content. As noted above, currently available HDCP protocols must be implemented using a DVI type connector.

[0017] The present invention provides a high definition high bandwidth copy protection protocol suitable for use in a packet based transmission medium that provides a robust digital copyright protection protocol that supports high definition copy protection that is backwards compatible with existing high definition copy protection protocols. In one embodiment of the invention the inventive HDCP protocol is carried out as a packet based high bandwidth copy protection method that includes forming a number of data packets at a source device, encrypting selected ones of the data packets based upon a set of encryption values, transmitting the encrypted data packets from the source device to a sink device coupled thereto, decrypting the encrypted data packets based in part upon the encryption values, and accessing the decrypted data packets by the sink device.

[0018] A particularly well suited packet based transmission system is described with reference to Fig. 1 that shows a generalized representation of a cross platform packet based digital video display interface 100 suitable for use with any embodiment of the invention. The interface 100 connects a transmitter 102 to a receiver 104 by way of a physical link 106 (also referred to as a pipe). In the described embodiment, a number of data streams 108 - 112 are received at the transmitter 102 that, if necessary, packetizes each into a corresponding number of data packets 114. These data packets are then

formed into corresponding data streams each of which are passed by way of an associated virtual pipe 116 - 120 to the receiver 104. It should be noted that the data streams 108 - 112 can take any number of forms such as video, graphic, audio, etc.

[0019] Typically, when the source is a video source, the data streams 108 - 112 include various video signals that can have any number and type of well-known formats, such as composite video, serial digital, parallel digital, RGB, or consumer digital video. The video signal can be an analog video signal provided the source 102 includes some form of an analog video source such as for example, an analog television, still camera, analog VCR, DVD player, camcorder, laser disk player, TV tuner, set top box (with satellite DSS or cable signal) and the like. The source 102 can also include a digital image source such as for example a digital television (DTV), digital still camera, and the like. The digital video signal can be any number and type of well known digital formats such as, SMPTE 274M-1995 (1920 x 1080 resolution, progressive or interlaced scan), SMPTE 296M-1997 (1280 x 720 resolution, progressive scan), as well as standard 480 progressive scan video.

[0020] In the case where the source 102 provides an analog image signal, an analog-to-digital converter (A/D) converts an analog voltage or current signal into a discrete series of digitally encoded numbers (signal) forming in the process an appropriate digital image data word suitable for digital processing. Any of a wide variety of A/D converters can be used. By way of example, other A/D converters include, for example those manufactured by: Philips, Texas Instrument, Analog Devices, Brooktree, and others.

[0021] For example, if the data stream 110 is an analog type signal, the an analog to digital converter (not shown) included in or coupled to the transmitter 102 will digitize the analog data which is then packetize by a packetizer that converts the digitized data stream 110 into a number of data packets 114 each of which will be transmitted to the receiver 104 by way of the virtual link 116. The receiver 104 will then reconstitute the data stream 110 by appropriately recombining the data packets 114 into their original format. It is these data streams that are ultimately encrypted for form a set of copy protected data streams.

[0022] Fig. 2 shows an encryption system 200 for encrypting audio/video content suitable for use with the system 100 described with respect to Fig. 1. As shown in Fig. 2, a video source 202 is arranged to provide a number of data streams such as the datastreams 110 and 112. By utilizing a number of data streams, the system 200 is capable of transmitting video data, for example, consistent with any of a number of video formats concurrently. For example, the data stream 110 is formed of video data consistent with 1024 x 768 at 60 Hz whereas the datastream 112 is formed of video data consistent with 640 x 480 at 75Hz, and so on. In order for a receiver 204 (such as a monitor) to reconstruct the video in the appropriate format, the datastreams include in addition the appropriate video data associated attribute data that is used by the receiver to reconstruct the video in the appropriate format.

[0023] Accordingly, the video source 202 includes a number of buffers 206 each of which is used to buffer an associated one of the video datastreams. Each of the buffers is, in turn, coupled to a multiplexer 208 that is used to select a particular one of the data streams for transmission to a packetizer 210. The packetizer 210 parses the incident data stream into an associated number of data packets by incorporating a packet ID, optionally performing error correction, and attaching a time stamp and any of the attributes deemed important or necessary for the correct reconstruction of the video raster by the receiver 404. An encryption control generator unit 212 applies an appropriate encryption algorithm to each of the data packets based at least by inserting a control packet that conveys signals such as H_{sync}, V_{sync}, and a particular control character CNTL3 used to flag those data packets that are encrypted (and conversely those data packets that are not encrypted).

[0024] In accordance with an embodiment of the invention, the resulting encrypted data stream 214 (a particular example of which is shown in Fig. 3 as a datastream 300) is formed of a number of data packets. The data stream 300 includes a number of control packets 302 used to mark those video data packets that are encrypted (or not encrypted) as the case may be. Each video packet has an associated header 304 that includes, in part, the attribute data described above associated with the video data packet 306. For example, in the case shown in Fig. 3, the data stream 300 includes data packets for the datastream 110 and the datastream 112 conjoined into the data stream 300 such that the traffic between the video source 202 and the receiver 204 is consistent with a constant link environment.

[0025] It should be noted that in the described embodiment, the data stream 300 is time domain multiplexed, those data packets associated with the datastream 110 have a longer duration than those associated with the data stream 112. In these cases, a time-base recovery (TBR) unit 216 within the receiver 204 regenerates the stream's original native rate using time stamps embedded in the main link data packets, if necessary. Referring back to Fig. 2, at the receiver 404, a deserializer unit 218 receives the encrypted datastream 300 that provides input to a decoder unit 220 and a depacketizer 222. The decoder 220 decodes the control packet, thus feeding H_{sync}, V_{sync}, and a particular control character CNTL3provided to a decryption engine 228 that was previously used to for encryption.

[0026] Fig. 4 illustrates a system 400 employed to implement the invention. Computer system 400 is only an example of a graphics system in which the present invention can be implemented. System 400 includes central processing unit (CPU) 410, random access memory (RAM) 420, read only memory (ROM) 425, one or more

peripherals 430, graphics controller 460, primary storage devices 440 and 450, and digital display unit 470. CPUs 410 are also coupled to one or more input/output devices 490 that may include, but are not limited to, devices such as, track balls, mice, keyboards, microphones, touch-sensitive displays, transducer card readers, magnetic or paper tape readers, tablets, styluses, voice or handwriting recognizers, or other well-known input devices such as, of course, other computers. Graphics controller 460 generates analog image data and a corresponding reference signal, and provides both to digital display unit 470. The analog image data can be generated, for example, based on pixel data received from CPU 410 or from an external encode (not shown). In one embodiment, the analog image data is provided in RGB format and the reference signal includes the V_{SYNC} and H_{SYNC} signals well known in the art. However, it should be understood that the present invention can be implemented with analog image, data and/or reference signals in other formats. For example, analog image data can include video signal data also with a corresponding time reference signal.

[0027] Although only a few embodiments of the present invention have been described, it should be understood that the present invention may be embodied in many other specific forms without departing from the the scope of the present invention. The present examples are to be considered as illustrative and not restrictive, and the invention is not to be limited to the details given herein, but may be modified within the scope of the appended claims along with their full scope of equivalents.

[0028] While this invention has been described in terms of a preferred embodiment, there are alterations, permutations, and equivalents that fall within the scope of this invention. It should also be noted that there are many alternative ways of implementing both the process and apparatus of the present invention. It is therefore intended that the invention be interpreted as including all such alterations, permutations, and equivalents as fall within the true scope of the present invention.

Claims

1. A packet based high bandwidth copy protection method comprising:

   forming a number of data packets at a source device;
   encrypting the data packets based upon a set of encryption values;
   transmitting the encrypted data packets from the source device to a sink device coupled thereto;
   decrypting the encrypted data packets based in part upon the encryption values; and
   accessing the decrypted data packets by the sink device.

2. A method as recited in claim 1, wherein the source device is a video source and wherein the sink device is a video display and wherein the number of data packets include some audio data packets and some video data packets.

3. A method as recited in claim 2, wherein the encryption/decryption control signals include a Vsync, an Hsync, and a CNTL3.

4. A method as recited in claim 3, wherein each of the data packets is associated with an particular control packet.

5. A method as recited in claim 4, wherein when the CNTL3 is active, then the corresponding data packet is encrypted and vice-versa.

6. A system for providing high bandwidth copy protection in a packet based system, comprising:

   a source unit arranged to provide a number of data packets;
   a sink unit coupled to the source unit arranged to receive the data packets from the source unit;
   an encryption unit coupled to the source unit arranged to encrypt selected ones of the data packets sent from the source unit to the sink unit;
   a decryption unit coupled to the sink unit arranged to decrypt the encrypted data packets; and
   an encryption/decryption values generator arranged to provide a set of encryption/decryption values used to encrypt and decrypt the appropriate data packets.

7. A system as recited in claim 6, wherein the source unit is an audio/video unit arranged to provide audio type data packets and/or video type data packets.

8. A system as recited in claim 7, wherein the sink unit is a display unit arranged to display processed ones of the video data packets.

9. A system as recited in claim 8, wherein the display unit includes a number of speakers arranged to transmit audio signals based upon processed ones of the audio data packets.

10. A system as recited in claim 9, wherein the set of encryption/decryption control signals include Vsynch, Hsynch corresponding to the video data packets.

11. A system as recited in claim 10, wherein the set of encryption/decryption control signal further includes CNTL3 to flag those data packets that are encrypted.

12. Computer program product for providing a packet based high bandwidth copy protection, comprising:

computer code for forming a number of data packets at a source device;
computer code for encrypting the data packets based upon a set of encryption values;
computer code for transmitting the encrypted data packets from the source device to a sink device coupled thereto;
computer code for decrypting the encrypted data packets based in part upon the encryption values;
computer code for accessing the decrypted data packets by the sink device; and
computer readable medium for storing the computer code.

13. Computer program product as recited in claim 12, wherein the source device is a video source and wherein the sink device is a video display and wherein the number of data packets include some audio data packets and some video data packets.

14. Computer program product as recited in claim 13, wherein the encryption control signals include a Vsync, an Hsync, and a CNTL3.

15. Computer program product as recited in claim 14, wherein each of the data packets is associated with an particular control value CNTL3.

16. Computer program product as recited in claim 15, wherein when the CNTL3 is active, then the corresponding data packet is encrypted and vice-versa.

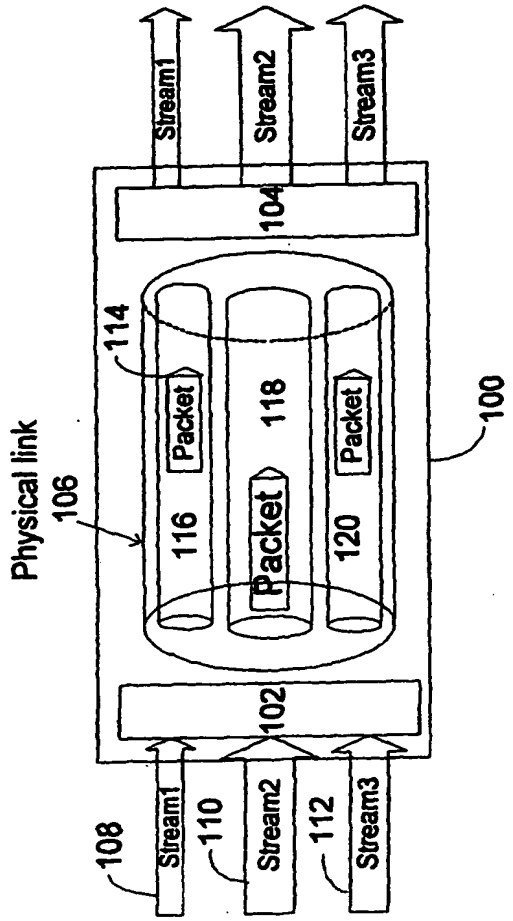
Stream1
Stream2
Stream3
104
114
Packet
118
Packet
Physical link
106
116
Packet
120
100
102
108
Stream1
110
Stream2
112
Stream3

Fig. 1

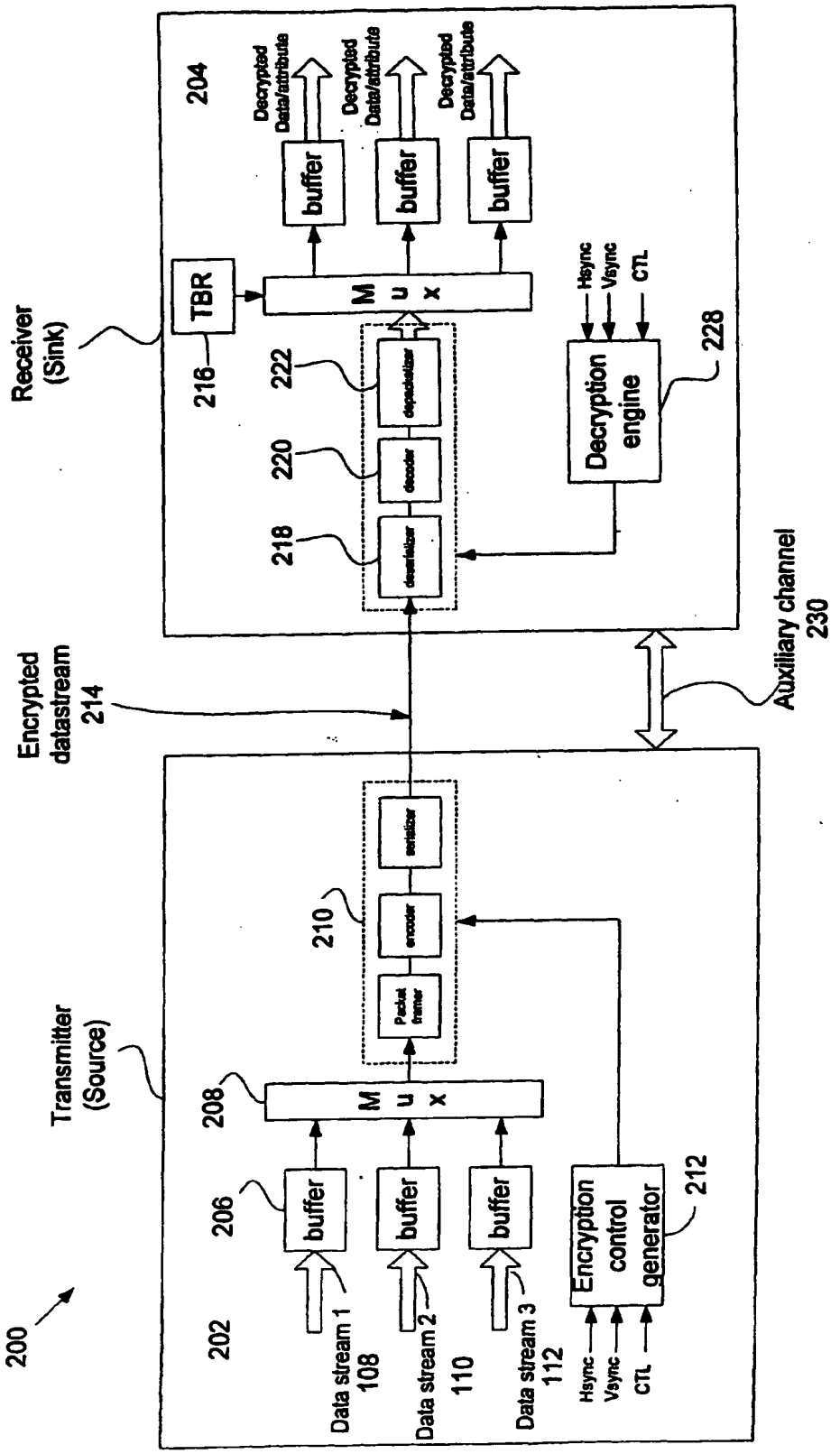
200
Transmitter (Source)
Receiver (Sink)
Encrypted datastream 214
Auxiliary channel 230
202
206
208
210
204
216
218
220
222
228
buffer
Mux
Packet framer
encoder
serializer
deserializer
decoder
TBR
Decryption engine
Encryption control generator
Data stream 1 108
Data stream 2 110
Data stream 3 112
Hsync
Vsync
CTL
Decrypted Data/attribute

Fig. 2

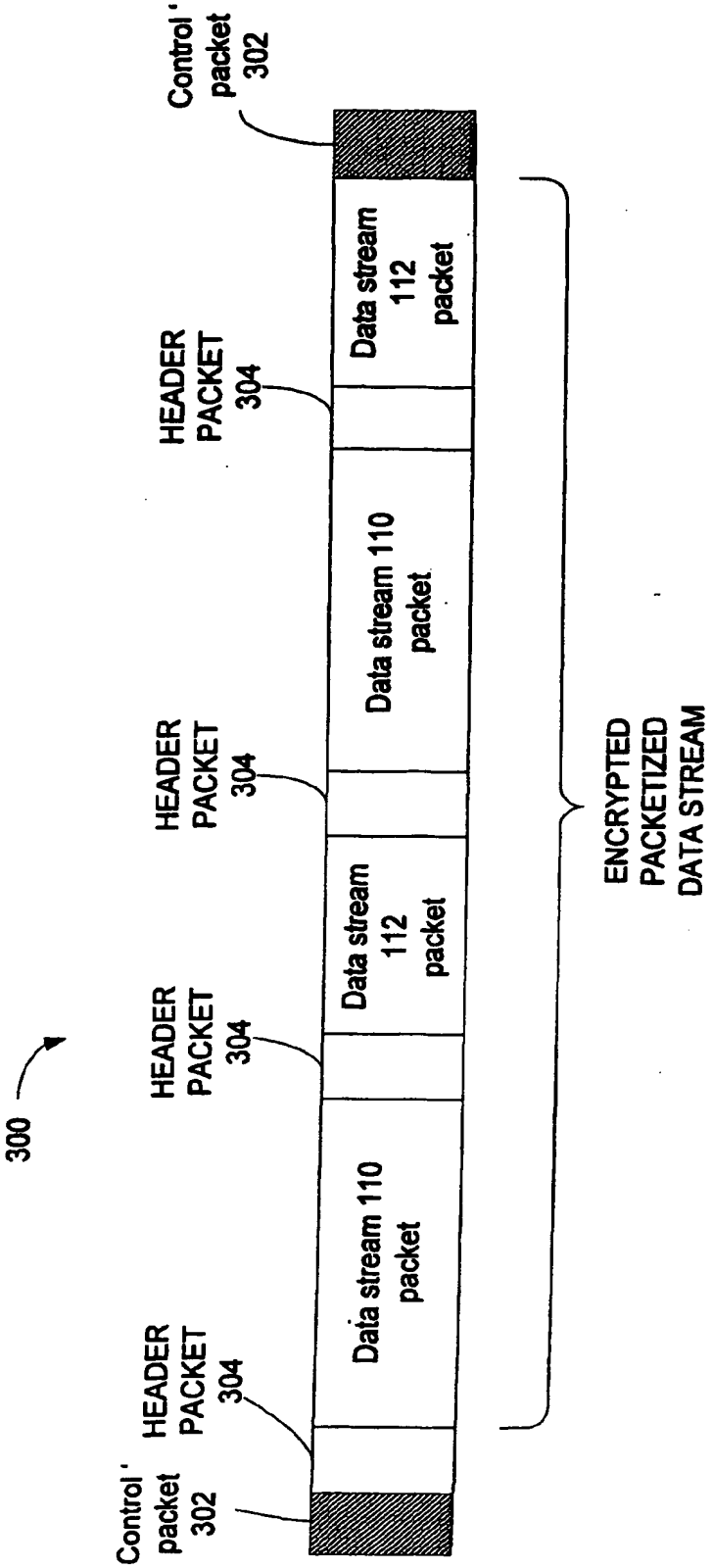
300
Control packet 302
HEADER PACKET 304
Data stream 110 packet
HEADER PACKET 304
Data stream 112 packet
HEADER PACKET 304
Data stream 110 packet
HEADER PACKET 304
Data stream 112 packet
Control packet 302
ENCRYPTED PACKETIZED DATA STREAM

Fig. 3

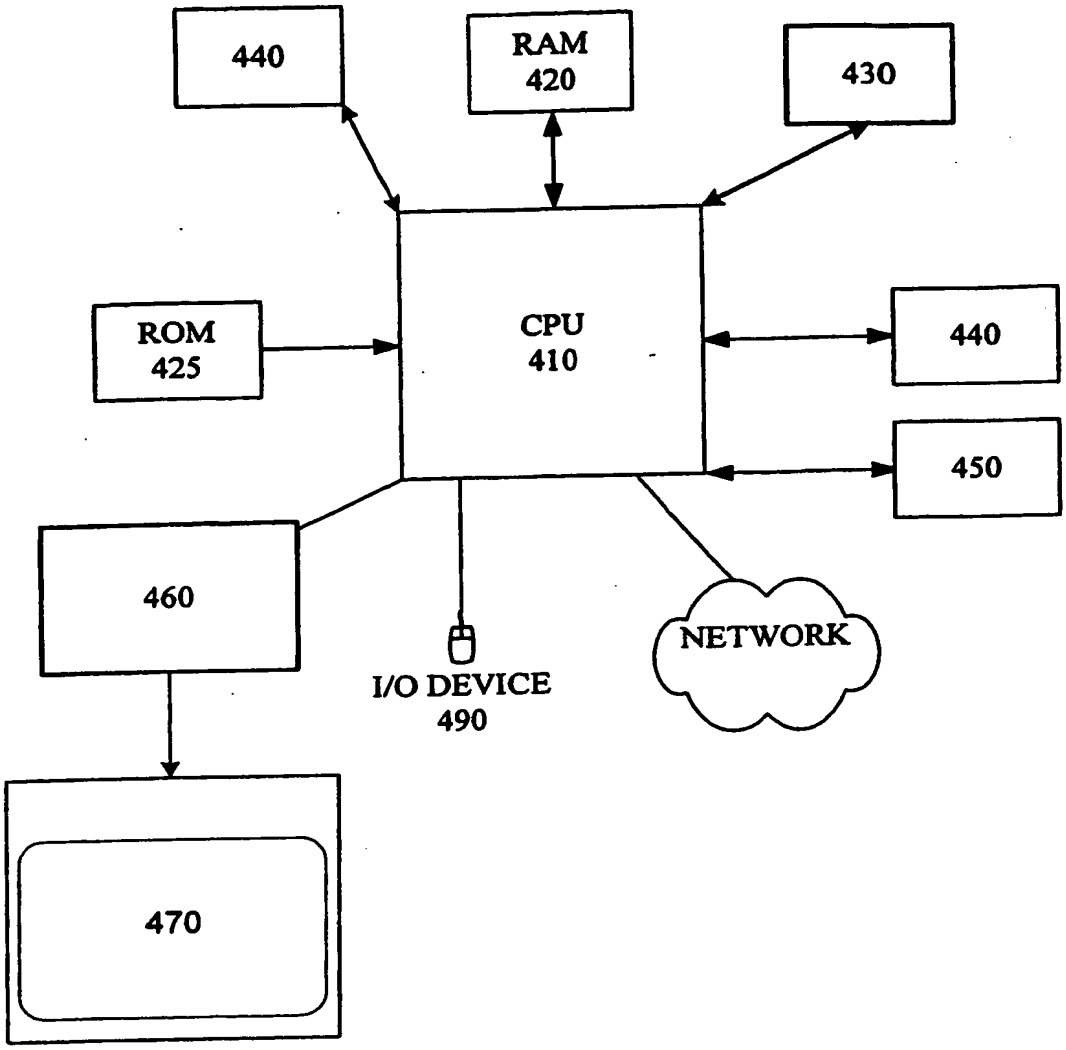
440
RAM
420
430
ROM
425
CPU
410
440
450
460
I/O DEVICE
490
NETWORK
470
400

Fig. 4